# Affine型合同反復模型の状態遷移図について(理論計算機科学とその周辺)

AUTHOR(S):

隈本, 覚; 乃美, 正哉

CITATION:

隈本, 覚 ...[et al]. Affine型合同反復模型の状態遷移図について(理論計算機科学とその周辺). 数理解析研究所講究録 1992, 790: 256-262

ISSUE DATE:

1992-06

URL:

http://hdl.handle.net/2433/82642

数理解析研究所講究録
256
第790巻 1992年 256-262

# Affine型合同反復模型の状態遷移図について

九大理　隈本覚　( Satoru Kumamoto )
九工大情報工　乃美正哉　( Masaya Nohmi )

## 1 はじめに

これまでに線形非線形を問わず様々なセルオートマトンが考えられてきた。本稿では藤野 [1] の定義した Affine 型の遷移写像を持つ合同型反復模型の挙動の解析手法と、その挙動を表現するグラフの表現方法を提案し、グラフの構造を決定する。

## 2 合同型反復模型の定義

$m$ を任意の自然数とする。ここで考える合同型反復模型とはシステム $K_{m,a,b} =< \mathbf{Z}_m, f >$ のことである。ただし、$\mathbf{Z}_m = \{0,1,2,\cdots,m-1\}$ であり、$f : \mathbf{Z}_m \to \mathbf{Z}_m$ は $f(x) = ax + b \mod m$ で与えられる。$\mathbf{Z}_m$ を状態集合、$x \in \mathbf{Z}_m$ を状態、$f$ を遷移写像という。

状態集合 $\mathbf{Z}_m$ は有限であるから、任意の $x \in \mathbf{Z}_m$ から得られる反復列 $\{f^k(x)\}_{k=0,1,2,\cdots}\}$ は、必ず有限回の反復の後に周期的な挙動をする。そこで、任意の状態からの反復をグラフ（状態遷移図と呼ぶ）に表すことが考えられる。最初に記号の定義をする。[1]

**定義 2.1** 模型 $K_{m_1,a_1,b_1} =< \mathbf{Z}_{m_1}, f_1 >$, $f_1(x) = a_1x + b_1 \mod m_1$ $(x \in \mathbf{Z}_{m_1})$ と、$K_{m_2,a_2,b_2} =< \mathbf{Z}_{m_2}, f_2 >$, $f_2(x) = a_2x + b_2 \mod m_2$ $(x \in \mathbf{Z}_{m_2})$ の積 $K_{m_1,a_1,b_1} \times K_{m_2,a_2,b_2}$ を次のように定義する。

$$K_{m_1,a_1,b_1} \times K_{m_2,a_2,b_2} =< \mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2}, f >$$

ただし、$f : \mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \to \mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2}$は、各 $x_1 \in \mathbf{Z}_{m_1}, x_2 \in \mathbf{Z}_{m_2}$に対して、次で与えられる。

$$f(x_1, x_2) = (f_1(x_1), f_2(x_2))$$

定義 **2.2** $K_{m,a,b}$に対して、その状態遷移図を与える写像を $G(K_{m,a,b})$ と表す。

定義 **2.3** 2つの模型 $K_{m_1,a_1,b_1}$と、$K_{m_2,a_2,b_2}$の状態遷移図 $G(K_{m_1,a_1,b_1})$ と、$G(K_{m_2,a_2,b_2})$ の積 $G(K_{m_1,a_1,b_1}) \times G(K_{m_2,a_2,b_2})$ を次のように定義する。

$$G(K_{m_1,a_1,b_1}) \times G(K_{m_2,a_2,b_2}) = G(K_{m_1,a_1,b_1} \times K_{m_2,a_2,b_2})$$

定義 **2.4** 2つの模型の状態遷移図 $G(K_{m_1,a_1,b_1})$ と $G(K_{m_2,a_2,b_2})$ がグラフとして同型のとき、

$$G(K_{m_1,a_1,b_1}) \cong G(K_{m_2,a_2,b_2})$$

と表す。

次に、合同型反復模型の状態遷移図 $G$ を具体的に表現する記号を定義する。

定義 **2.5** 具体的なグラフを表す記号を以下のように定義する。

(1) $< l >$とは、位数が $l$のサイクルを表す。(各頂点のラベルは 1 である。)

(2) Tree の各 node にラベルをつける。(ラベルの付け方は次の例を参照)

(3) $[b]$ とは高さ 1 の Tree を表す記号で、高さ 1 の点にラベル 2 から $b$ がついていて、そこから Tree の根 (ラベル 1 がついている) への辺があることを示す。

(4) $[b_1][b_2|b_1]$ とは、高さ 2 の Tree を表す記号で、$[b_1]$ の高さ 1 の頂点で、ラベルが $b_2$以下のものについては、全て $b_1$分岐しているものである。(高さ 1 の) 同じ頂点から分岐した高さ 2 の各頂点には、それぞれラベル 1 から $k$をつける。

(5) 以下同様にして、$[b_1][b_2|b_1]\cdots[b_k|b_{k-1}|\cdots|b_1]$ を定義する。

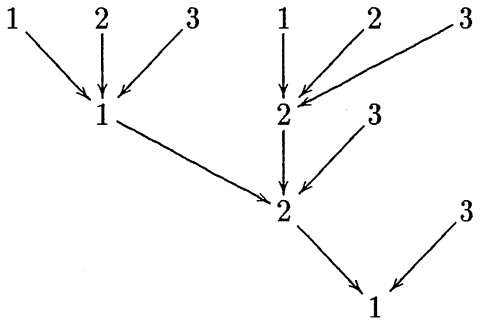
(6) $[b_1|b_2|\cdots|b_k]^k = [b_1][b_2|b_1]\cdots[b_k|b_{k-1}|\cdots|b_1]$ とする。

(7) $< l > [b_1|b_2|\cdots|b_k]^k(n)$ とは、位数 $l$のサイクルの各頂点の上に $\mathrm{Tree}[b_1|b_2|\cdots|b_k]^k$があるグラフが $n$ 個存在することを示す。

注意 $< 1 > [b_1|b_2|\cdots|b_k]^k$のことを $[b_1|b_2|\cdots|b_k]^k$、$[b_2|b_2|b_2|b_1]$ のことを $[[b_2]^3|b_1]$ 等と書くことがある。

例 **2.6**

$$[3|2|2]^3 \cong [3][2|3][2|2|3]$$




定義 **2.7** 記号 $b_1 \to b_2 \to \cdots \to 1$ とは、グラフ上の頂点を表す記号で、高さ $n$ の点のうちで根までの経路上の点についたラベルが上から順に $b_1, b_2, \cdots, 1$ となる点を示す。

注意 上の記号で、最も右にある 1 は常にグラフの根の部分を表すことにする。

# 3 合同型反復模型の解析

次に、任意の合同型反復模型の解析手法について考える。

定義 **3.1** $p$ を素数、$x \in \mathbf{Z}_{p^r}$とする。$x \neq 0$ のとき、$p^i|x$ を満たす最大の $i$ を$\nu_p(x)$ と書く。
$x = 0$ のとき、$\nu_p(0) = r$とする。

解析に用いる以下の定理が藤野 [1] によって与えられている。

定理 **3.2** 二つの模型 $K_{m,a,0} =< \mathbf{Z}_m, f >, K_{m,a,b} =< \mathbf{Z}_m, f' > \quad (b \neq 0)$ について、

$$G(K_{m,a,0}) \cong G(K_{m,a,b})$$

であるための必要十分条件は、$f'$が $\mathbf{Z}_m$で、不動点を持つことである。

定理 **3.3** $a = 0$ のとき、

$$G(K_{p^r}, a, b) \cong < 1 > [p^r](1)$$

定理 **3.4** $a = 1$ のとき、

$$G(K_{p^r}, a, b) \cong < p^{r-\nu_p(b)} > (p^{\nu_p(b)})$$

定理 **3.5** $m \in \mathbf{N}$ $(m \geq 2)$ が $m = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$ と素因数分解されるとき

$$G(K_{m,a,b}) \cong G(K_{p_1^{r_1},a,b}) \times \cdots \times G(K_{p_s^{r_s},a,b})$$

が成立する。

よって、$G(K_{p^r}, a, b)$ を決定し、グラフの積の作り方を考えればよい。

## 3.1 $\nu_p(a) \geq 1$ のとき。

$G(K_{p^r,a,b})$ を考える。$\nu_p(a) \geq 1$ より $(a-1, p) = 1$ なので、$x = ax + b \mod p^r$ は $\mathbf{Z}_{p^r}$ 中に解を持つ。つまり、$K_{p^r,a,b}$は不動点を持つので、$K_{p^r,a,0}$ のみを考えればよい。

$G(K_{p^r,a,0})$ について、以下のことがわかる。

- 不動点は 0 のみである。
- 分岐は存在すれば $p^{\nu_p(a)}$分岐である。
- $r = r'\nu_p(a) + r'' \ (0 \leq r'' < \nu_p(a))$ とすれば、Tree の高さは $\begin{cases} r' & (r'' = 0) \\ r'+1 & (r'' \neq 0) \end{cases}$ である。

以上をまとめると、以下の定理が成り立つ。

定理 **3.6** $\nu_p(a) \geq 1$、$r = r'\nu_p(a) + r''$のとき、

$$\begin{aligned} r'' = 0 \Rightarrow G(K_{p^r,a,b}) &\cong [[p^{\nu_p(a)}]^{r'}]^{r'} \\ r'' \neq 0 \Rightarrow G(K_{p^r,a,b}) &\cong [[p^{\nu_p(a)}]^{r'} | p^{r''}]^{r'+1} \end{aligned}$$

### 3.2 $\nu_p(a)=0$ かつ$\nu_p(a-1)<\nu_p(b)$ のとき。

$\nu_p(a-1)\leq\nu_p(b)$ のときは、不動点 $x=-b/(a-1)$ が存在するので、$K_{p^r,a,0}$のみを考えればよい。

定義 **3.7** 集合 $N_i$を以下のように定義する。

$$N_i=\{x\in\mathbf{Z}_{p^r}|\nu_p(x)=i\}\ (0\leq i\leq r-1)$$

定義から直ちに、次が成立する。

命題 **3.8** 上の $N_i$に対して、以下の3つが成立する。

- $\mathbf{Z}_{p^r}=\cup_{i=0}^{r-1}N_i$
- $\#N_i=(p-1)p^{r-i-1}$
- $G(K_{p^r,a,0})\cong\cup_{i=0}^{r-1}G(K_{N_i,a,0})$

定義 **3.9** $a$ の $\mathbf{Z}_p^{r-i}$における乗法位数を$\mu_i(a)$ と書く。

定理 **3.10** $K_{N_i,a,0}$の状態遷移グラフ $G(K_{N_i,a,0})$ は、次で与えられる。

$$G(K_{N_i,a,0})\cong<\mu_i(a)>\left(\frac{\varphi(p^{r-i})}{\mu_i(a)}\right)$$

ただし、$\varphi$ はオイラー関数で、$\varphi(p^{r-i})=(p-1)p^{r-i-1}$である。

### 3.3 $\nu_p(a)=0$ かつ$\nu_p(a-1)>\nu_p(b)$ のとき。

$a=1$ についてはよいので、$a\neq1$ とする。

$$f^n(x)=a^nx+\frac{a^n-1}{a-1}b$$

であるから、

$$f^n(x)=x\iff(a^n-1)x+\frac{a^n-1}{a-1}b=0$$

となる。この計算を $\mathbf{Z}$ で行うと、

$$\nu_p((a^n-1)x+\frac{a^n-1}{a-1}b)\geq r\qquad(1)$$

上の式を満たすような最小の $n$ を見つければよい。

$$\begin{aligned}\nu_p((a^n-1)x) &= \nu_p(a^n-1)+\nu_p(x)\\ \nu_p\left(\frac{a^n-1}{a-1}\right) &= \nu_p(a^n-1)+\nu_p(b)-\nu_p(a-1)\end{aligned}$$

であり、条件から$\nu_p(b)-\nu_p(a^n-1)<0\leq\nu_p(x)$ よって式 (1) は、次と同値。

$$\nu_p(a^n-1)+\nu_p(b)-\nu_p(a-1)\geq r \tag{2}$$

$a=1+a'p^{\nu_p(a-1)}$と書けるので、$a^n=1+a'np^{\nu_p(a-1)}+\cdots$ よって、次が成立する。

$$\nu_p(a^n)=\nu_p(a-1)+\nu_p(n)$$

従って式 (2) は$\nu_p(n)+\nu_p(b)\geq r$と同値となる。以上から、$n=p^{r-\nu_p(b)}$が式 (1) を満たす最小の自然数である。つまり、サイクルの長さは $p^{r-\nu_p(b)}$ である。
まとめると以下の定理となる。

定理 **3.11** $\nu_p(a)=0$ かつ$\nu_p(a-1)>\nu_p(b)$ のとき次が成立する。

$$G(K_{p^r,a,b})\cong<p^{r-\nu_p(b)}>(p^{\nu_p(b)})$$

# 4 グラフの積について

これまでで、構造が簡単な場合の状態遷移グラフの作り方がわかった。この節では、与えられたこのタイプの 2 つのグラフの積を決定する。

定理 **4.1** $T'=[b_1|b_2|\cdots|b_k]^k$ , $T''=[c_1|c_2|\cdots|c_k]^k$ $T=[b_1c_1|b_2c_2|\cdots|b_kc_k]^k$ とおくと

$$T'\times T''\cong T$$

が成立する。

$k>k'$のとき明らかに $[b_1|b_2|\cdots|b_{k'}]^{k'}\cong[b_1|b_2|\cdots|b_{k'}|[1]^{k-k'}]^k$であるから次の次の系が成り立つ。

系 **4.2** $k>k'$のとき、

$$[b_1|b_2|\cdots|b_k]^k\times[c_1|c_2|\cdots|c_{k'}]^{k'}\cong[b_1c_1|b_2c_2|\cdots|b_{k'}c_{k'}|b_{k'+1}|\cdots|b_k]^k$$

サイクル同士のグラフの積等についても考えて全てまとめると以下の定理となる。

定理 **4.3** $B_1 = [b_{1,1}|\cdots|b_{1,k_1}]^{k_1}$ , $B_2 = [b_{2,1}|\cdots|b_{2,k_2}]^{k_2}$ とおくと次が成り立つ。

$$< l_1 > B_1(n_1) \times < l_2 > B_2(n_2) \cong < \mathrm{lcm}(l_1, l_2) > B_1 \times B_2(\gcd(l_1, l_2) n_1 n_2)$$

# 参考文献

[1] 藤野 精一 ; $n$ 元連立 1 次合同型反復模型とその挙動解析,RMC 64-09J(1989) 九州大学数学教室